Tienda Wifi

CiudadWireless es la tienda Wifi recomendada por elhacker.NET

Tutoriales y Manuales

- Recopilación de **Tutoriales y Manuales** ordenados por categorías
- **Descargas** Cursos, Tutoriales y Manuales, Libros PDF

Entradas Mensuales

- ► 2022 (Total: 630)
- ► 2021 (Total: 730)
- ► 2020 (Total: 212)
- ► 2019 (Total: 102)
- ► 2018 (Total: 150)
- ▼ 2017 (Total: 231)
  - ► diciembre (Total: 10)
  - ► noviembre (Total: 21)
  - ► octubre (Total: 14)
  - ► septiembre (Total: 16)
  - ► julio (Total: 6)
  - ▼ junio (Total: 21)
    - **Encuentran fallo en el microcódigo de los procesad...**
    - **Dos personas arrestadas en Inglaterra por acceder ...**
    - **Cinco alumnos detenidos por hackear correos de pro...**
    - **El gobierno mexicano utiliza software espía contra...**
    - **La Unión Europea quiere hacer obligatorio el uso d...**
    - **GPS para montañeros: OruxMaps**
    - **Marea: el cable de fibra óptica de mayor capacidad...**
    - **Cherry Blossom: la herramienta de la CIA para hack...**
    - **El fundador de Telegram asegura que el FBI le ofre...**
    - **Novedades del software libre: Nmap, WordPress, Fir...**
    - **Actualizaciones de seguridad para productos Adobe ...**
    - **Solo el 8% de las chicas de 15 años quiere estudia...**
    - **Disponible Tor Browser 7.0**
    - **Primer malware que utiliza vulnerabilidad en Intel AMT**
    - **Malware en PowerPoint sin usar Macros, JScript o V...**
    - **Múltiples y graves vulnerabilidades en cámaras IP d...**
    - **El rastro de una impresora delata a la persona que...**
    - **La justicia alemana niega a unos padres el acceso ...**
    - **250 millones de ordenadores infectados por el malw...**
    - **Cancelan crowdfunding para comprar exploits de la ...**
    - **¿El sobrecalentamiento de un iPhone es la causa de...**
  - ► mayo (Total: 10)
  - ► abril (Total: 31)
  - ► marzo (Total: 39)
  - ► febrero (Total: 36)
  - ► enero (Total: 27)
- ► 2016 (Total: 266)
- ► 2015 (Total: 445)
- ► 2014 (Total: 185)
- ► 2013 (Total: 100)
- ► 2012 (Total: 8)
- ► 2011 (Total: 7)
- ► 2010 (Total: 15)

Síguenos en:

Suscripción

¿Quieres recibir las últimas novedades del blog en tu correo?

¡Suscríbete al feed!

Ingresar email aquí | OK

BY FEEDBURNER

- Rusia contrató a trolls para difundir propaganda a favor de la invasión de Ucrania, dice Meta
- Continúa la crisis en los semiconductores por la tensión entre Taiwán y China
- Así puedes rellenar cualquier PDF bajado de Internet sin problemas
- Así infectan tu PC con virus ahora que no pueden usar Word y Excel
- Si tienes esta extensión en Chrome han leído todos tus correos de Gmail

Blogroll

- Flu Project
- Security At Work
- We Live Security
- Blog Segu-Info
- HackPlayers
- TheHackerWay
- CyberHades
- La9deAnon
- DerechoDeLaRed
- Snifer@L4b's
- BandaAncha
- ugeek
- ochobitshacenunbyte

Etiquetas

noticias (396) seguridad (359) privacidad (284) ransomware (224) vulnerabilidad (209) google (192) android (191) software (189) Malware (184) Windows (170) tutorial (170) cve (156) manual (155) hardware (144) linux (98) ddos (73) herramientas (71) Wifi (69) hacking (68) sysadmin (59) app (58) cifrado (56) WhatsApp (54) twitter (54) nvidia (36) Networking (34) firmware (34) ssd (32) adobe (31) eventos (30) office (30) firefox (29) antivirus (28) cms (28) contraseñas (28) flash (26) hack (26) youtube (25) MAC (24) programación (23) anonymous (22) juegos (19) apache (18) exploit (18) multimedia (18) Kernel (17) SeguridadWireless (17) javascript (17) ssl (17) documental (16) conferencia (14) Debugger (13) Forense (13) técnicas hacking (13) auditoría (12) lizard squad (12) delitos (11) Virtualización (10) metasploit (10) adamo (9) reversing (9) Rootkit (8) Ehn-Dev (7) antimalware (6) MAC Adress (5) oclHashcat (5)

Entradas populares

Filtran 4TB datos empresa israelí Cellebrite, especializada en desbloquear iPhones

Una fuente anónima filtra 4 TB de datos de Cellebrite después de un ataque cibernético. En España Cellebrite logró desbloquear el iPhone 6 ...

¿En qué consiste el SIM swapping? Consejos para evitarlo y detectarlo

El SIM swapping, o el intercambio de SIM en castellano, es un método en el que los ciberdelincuentes consiguen un duplicado de la tarjeta S...

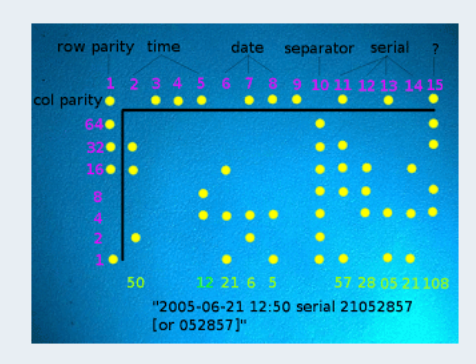
Mítico reproductor música MP3 WinAmp está de vuelta

Winamp está de vuelta. Esta vez de verdad. El reproductor que marcó la adolescencia de toda una generación, se adapta a los tiempos del st...

El rastro de una impresora delata a la persona que filtró documentos confidenciales

miércoles, 7 de junio de 2017 | Publicado por el-brujo

El problema es que la mayoría de las nuevas **impresoras imprimen casi de forma invisible unos** puntos amarillos **que rastrean exactamente cuándo y dónde se imprimen documentos**, cualquier documento. Los llamados "Tracking Dots". Esos puntos indican el número de serie y modelo de la impresora, **además de la fecha y hora exacta de la impresión**. Debido a que **la NSA registra todos los trabajos de impresión en sus impresoras**, puede utilizar esto para coincidir exactamente con quién imprimió el documento.



Cuando las **impresoras** empezaron a popularizarse en los hogares en los años 80, el gobierno de Estados Unidos empezó a preocuparse de que pudieran empezar a imprimirse falsificaciones de dinero y otro tipo de documentos. Por ello, se desarrolló un sistema que estuvo oculto durante 20 años, y todavía sigue presente en la mayoría de impresoras.

Puntos de seguimiento en Impresoras - Machine Identification Code (MIC)

Este sistema es conocido oficialmente como **Machine Identification Code (MIC)**, aunque comúnmente se le llama "**puntos amarillos**". Estos puntos son una **marca de agua** que las impresoras láser incluyen en los documentos que imprimen. El sistema fue desarrollado por **Xerox y Canon** a mediados de los años 80, y su existencia fue descubierta en 2004 después de saliera a la luz una noticia de que las autoridades de Países Bajos consiguieran atrapar a unos falsificadores de dinero que habían usado impresoras Canon a través de "una función oculta en las impresoras láser a color".

Durante décadas, las impresoras láser en color han rastreado invisiblemente a sus usuarios al incluir patrones de pequeños puntos amarillos en cada página de salida. Este seguimiento fue conocido por las personas que trabajaron en la industria de la imagen y fue intermitentemente revelado por algunos fabricantes en su documentación. Pero incluso hoy en día, la mayoría de los usuarios finales no son conscientes de ello.

Esta semana The Intercept publicó un artículo en el que se hablaba de cómo las elecciones del año pasado en Estados Unidos **sufrieron ciberataques por parte de la inteligencia militar rusa**.

El FBI ha detenido a Reality Leigh Winner por filtrar Secretos de Estado. Al parecer, esta persona hizo llegar a los medios datos que **daban fuertes indicios** de que Rusia intentó hackear las elecciones estadounidenses en las que Donald Trump fue elegido presidente.

La responsable de la filtración ha sido arrestada. La joven de 25 años llamada Reality Leigh Winner ha sido identificada como la supuesta soplona, y para encontrarla la NSA ha estudiado (entre otras cosas) **un rastro invisible que dejan las impresoras** al imprimir documentos.

Se publicó la orden de arresto de un contratista de la NSA llamado "Reality Winner", mostrando cómo la localizaron porque ella había impreso los documentos y los había enviado a The Intercept. El documento publicado por The Intercept no es el PDF original, sino un PDF que contiene las imágenes de la versión impresa que fue escaneada más tarde.

En el documento filtrado esos puntos indicaban el número de serie y modelo de la impresora, **además de la fecha y hora exacta de la impresión**. Con esos datos la NSA pudo estudiar qué empleados tuvieron acceso a la impresora en esa fecha. Seis personas que trabajaban para la agencia gubernamental habían utilizado esa impresora, y los interrogatorios acabaron dando con Winner como la causante de esa filtración.

Winner fue arrestada el pasado sábado, justo antes de que el artículo apareciera en The Intercept este lunes. La responsable de la filtración **tenía acceso a documentos confidenciales** como miembro en activo de la Fuerza Aérea, y llevaba trabajando desde febrero de este año en las instalaciones de Pluribus International en Georgia. Ahora se enfrenta a una acusación por la recolección transmisión o pérdida de documentos de defensa.

Según documentos clasificados publicados por The Intercept y obtenidos de la NSA, **Rusia intentó hackear a al menos un proveedor de software de las máquinas de votación** utilizadas en las elecciones de Estados Unidos y también realizó más de cien ataques de spear-phishing (phishing orientado a conseguir acceso a datos confidenciales) dirigidos a funcionarios involucrados en el proceso electoral.

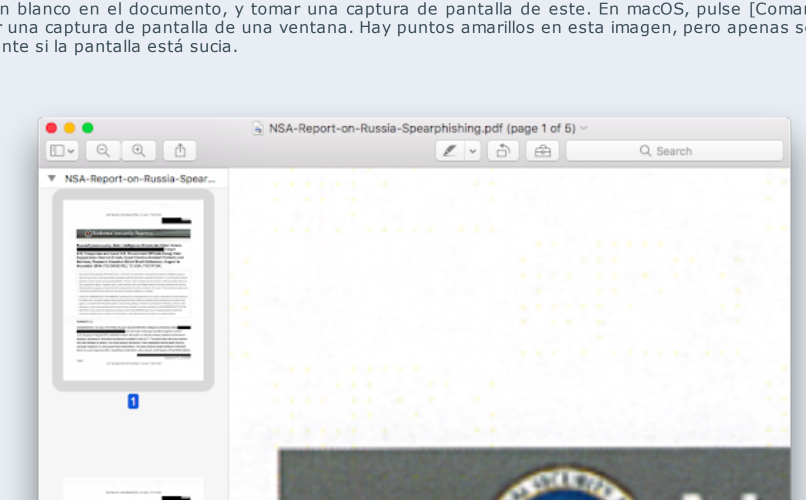
En Errata Security de Robert Graham lo explican y detallan cómo funciona ese sistema que no todo el mundo conoce y que permite "analizar" un documento impreso para **descubrir con qué tipo de impresora se ha imprimido**. La mayoría de las impresoras modernas hacen uso de los llamados "Tracking Dots", una serie de puntos que se pueden descubrir si uno hace una ligera edición del documento e invierte los colores.

En este post, se muestra cómo.

Puede descargar el documento del artículo original aquí:

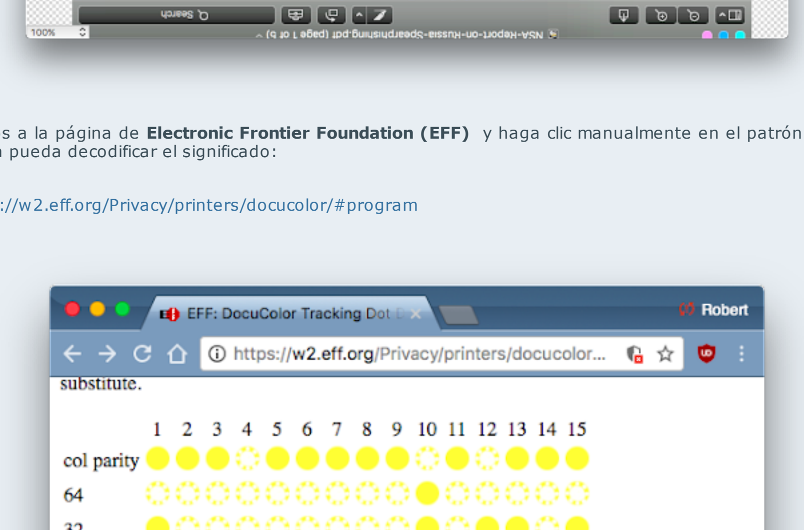
- https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/
- https://assets.documentcloud.org/documents/3766950/NSA-Report-on-Russia-Spearphishing.pdf

A continuación, puede abrirlo en un visor de PDF, como la aplicación "Vista previa" normal en macOS. Zoom en algunos espacios en blanco en el documento, y tomar una captura de pantalla de este. En macOS, pulse [Comando-Mayús-3] para tomar una captura de pantalla de una ventana. Hay puntos amarillos en esta imagen, pero apenas se pueden ver, especialmente si la pantalla está sucia.



Tenemos que resaltar los puntos amarillos. Abre la captura de pantalla en un editor de imágenes, como el programa "Pincel" integrado en macOS. Ahora utilice la opción "**Invertir colores**" en la imagen, para obtener algo como esto. Debes ver un tablero de damas de un patrón aproximadamente rectangular en el espacio en blanco.

Está al revés, así que tenemos que girarlo 180 grados, o flip-horizontal y flip-vertical:



Ahora vamos a la página de **Electronic Frontier Foundation (EFF)** y haga clic manualmente en el patrón para que su herramienta pueda decodificar el significado:

- https://w2.eff.org/Privacy/printers/docucolor/#program

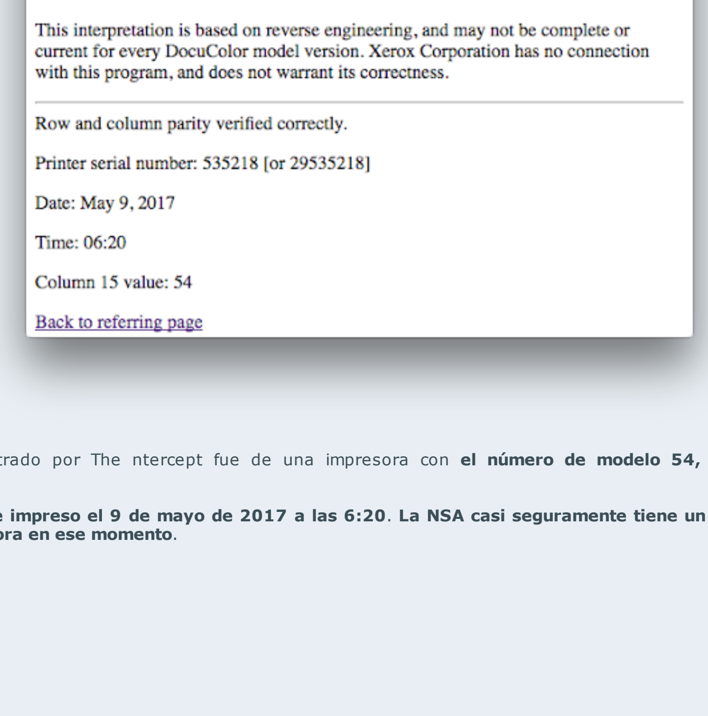
La EFF creó un listado con los modelos de impresoras que imprimen puntos amarillos

Posteriormente, la Electronic Frontier Foundation (EFF) pidió al público muestras de impresiones para encontrar patrones en el código y posteriormente descodificarlo. Así fue como consiguieron determinar qué significaban esos puntos amarillos que son sólo visibles con una luz intensa sobre el papel (si es ultravioleta mejor) y usando una lupa. Si no tienes una lupa, puedes imprimir un documento y luego escanear una pequeña parte de él a la mayor resolución que puedas. Posteriormente, se puede aumentar el canal de color amarillo para resaltar esos puntos.

En los últimos dos años, la **Electronic Frontier Foundation (EFF)** ha examinado este mecanismo de seguimiento -un sistema de interés ejemplar debido a la forma no transparente en que los gobiernos parecen haber persuadido a las empresas de tecnología a cambiar su diseño de producto sin ninguna base jurídica específica - y, con la ayuda de muchos voluntarios, hemos aprendido a leer algo de la información oculta.

Esta investigación está en curso, pero ya sabemos cómo hacer que los puntos sean fácilmente visibles (con luces LED, microscopios o escáneres de color ordinarios), y sabemos cómo leer los datos incorporados por varios fabricantes importantes de impresoras. Normalmente, una impresora marcará sus páginas de salida con el número de serie de la impresora y la fecha y hora en que se imprimió la página (si la impresora tiene su propio reloj incorporado). Esta información facilita asociar la salida de impresión en color con individuos, ya que podría correlacionarse con registros de tarjetas de crédito, registros de servidores, imágenes de cámaras de vigilancia y similares.

Esto produce el siguiente resultado:



El documento filtrado por The ntercept fue de una impresora con **el número de modelo 54, número de serie 29535218.**

El documento **fue impreso el 9 de mayo de 2017 a las 6:20**. **La NSA casi seguramente tiene un registro de quién utilizó la impresora en ese momento**.

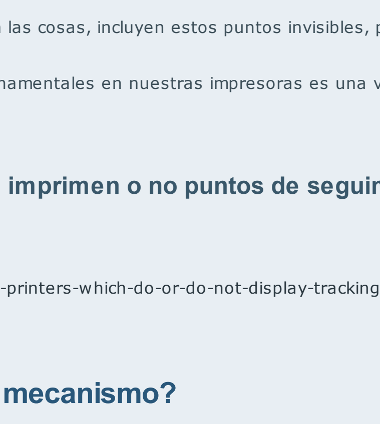
La situación es similar a cómo **Vice descubrió la ubicación de John McAfee, publicando fotografías JPEG de él con las coordenadas EXIF GPS metadatos aún ocultas en el archivo**.

Es importante tener en cuenta que el **FBI y la NSA no necesitaban saber que las páginas habían sido impresas**. **Todo el material clasificado como "top secret" (la máxima clasificación de seguridad que un documento puede recibir) se almacena en una intranet gubernamental masiva conocida como Joint Worldwide Intelligence Communications System, o JWICS.** Este sistema **registra a todos los que acceden a documentos secretos, así como lo que hacen con ellos**. Incluso si The Intercept hubiera verificado el documento sin alertar a la NSA, y después parafraseado el informe entero, después de que publicara su historia, el gobierno se habría movido rápidamente para determinar quién había accedido al documento - y Winner, eventualmente, estaría bajo el El mismo escrutinio.

O es la forma en que los archivos PDF a menudo se eliminan añadiendo una barra negra sobre la imagen, dejando el contenido subyacente en el archivo para que la gente pueda leer, como en este accidente de NYTime con un documento de Snowden. O cómo abrir un documento de Microsoft Office, y luego guardarlo accidentalmente, deja las huellas dactilares identificándolo detrás, como sucedió repetidamente con las filtraciones de la elección de Wikileaks. Este tipo de fallos son comunes con fugas.

Para **solucionar** este problema del punto amarillo**, utilice una impresora en blanco y negro, un escáner en blanco y negro o bien, lo puede convertir en blanco y negro con un editor de imágenes.**

Las impresoras tienen dos características puestas allí por el gobierno para ser malo para usted. La primera es que reconocen un patrón apenas visible en la moneda, por lo que no se puede utilizar para falsificar dinero, como se muestra en este $ 20 a continuación:



La segunda es que cuando imprimen las cosas, incluyen estos puntos invisibles, por lo que los documentos pueden ser rastreados.

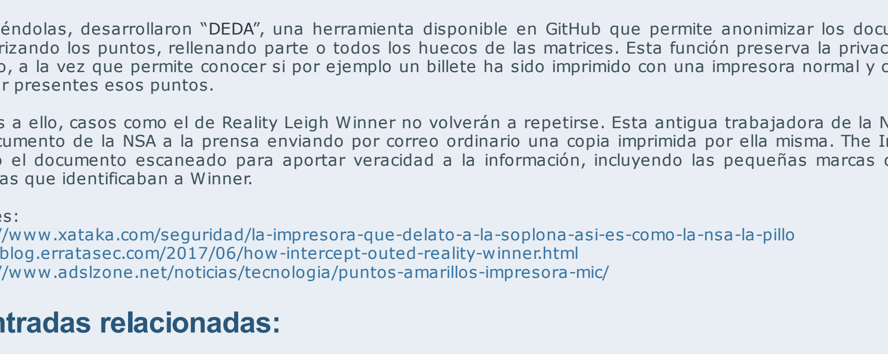
Sí, este código de las fuerzas gubernamentales en nuestras impresoras es una violación de nuestros derechos de la 3 ª Enmienda.

Listado de impresoras que imprimen o no puntos de seguimiento:

- https://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots

¿Es posible saltarse el mecanismo?

Por suerte, sí. En 2018, un grupo de investigadores desarrolló un software para anonimizar las impresiones y así **preservar la privacidad** de aquellos que hacen denuncias anónimas, así como activistas o periodistas. En la investigación analizaron los patrones de 106 modelos de impresoras de 18 fabricantes diferentes, y encontraron cuatro formas de codificar la información diferentes.



Conociéndolas, desarrollaron "DEDA", una herramienta disponible en GitHub que permite anonimizar los documentos aleatorizando los puntos, rellenando parte o todos los huecos de las matrices. Esta función preserva la privacidad del usuario, a la vez que permite conocer si por ejemplo un billete ha sido imprimido con una impresora normal y corriente al estar presentes esos puntos.

Gracias a ello, casos como el de Reality Leigh Winner no volverán a repetirse. Esta antigua trabajadora de la NSA filtró un documento de la NSA a la prensa enviando por correo ordinario una copia imprimida por ella misma. The Intercept publicó el documento escaneado para aportar veracidad a la información, incluyendo las pequeñas marcas de agua amarillas que identificaban a Winner.

Fuentes:
https://www.xataka.com/seguridad/la-impresora-que-delato-a-la-soplona-asi-es-como-la-nsa-la-pillo
http://blog.erratasec.com/2017/06/how-intercept-outed-reality-winner.html
https://www.adslzone.net/noticias/tecnologia/puntos-amarillos-impresora-mic/

Entradas relacionadas:

Guía NSA sobre la protección de las comunicaciones unificadas y los sistemas de voz y...

Vulnerabilidad es de la tecnología 5G

China utilizó un exploit 0-Day de la NSA años antes de que se hiciera público

La NSA publica el top 25 de vulnerabilidad es aprovechadas por los hackers Chinos

Espionaje internacional de la CIA durante años utilizando máquinas de cifrado suizas ...

Ex ingeniero de la CIA condenado por filtrar secretos de hacking de Vault 7 a Wikilea...

Etiquetas: espionaje , filtraciones , impresoras , nsa , tracking dots , USA. elecciones

0 comentarios :

PUBLICAR UN COMENTARIO

Los comentarios pueden ser revisados en cualquier momento por los moderadores.

Serán publicados aquellos que cumplan las siguientes condiciones:
- Comentario acorde al contenido del post.
- Prohibido mensajes de tipo SPAM.
- Evite incluir links innecesarios en su comentario.
- Contenidos ofensivos, amenazas e insultos no serán permitidos.

Debe saber que los comentarios de los lectores no reflejan necesariamente la opinión del STAFF.

Entrada más reciente | Inicio | Entrada antigua

Copyleft © 2010-2022. Blog de elhacker.NET. Algunos derechos reservados.
Usamos Cookies propias y de terceros. Consulta el Aviso Legal para más información.
Los contenidos de este blog están sujetos a una licencia Creative Commons a menos que se indique lo contrario.